



## Integrating External Captive Portal with On-Premise cnMaestro API



---

## Table of contents

### Chapter 1 Contents

---

|  |   |
|--|---|
| Introduction.....  | 3 |
| Feature Details .....  | 3 |
| Workflow.....  | 4 |
| 3 <sup>rd</sup> party certificate loading on cnMaestro: .....                                      | 5 |
| Configuration .....  | 7 |
| For deployments where cnMaestro hostname entry cannot be added to the DNS Server forward zone..... | 9 |

---

## Introduction

---

**Guest access WLAN** is designed specifically for BYOD (Bring your own device) setup, where large organizations have both staff and guests running on same WLAN or similar WLANs. Cambium Networks Provides different options to the customers to achieve this based on where the **captive portal page is hosted** and **who will be validating and performing authentication process**.

They are 3 locations where the captive portal page can be hosted:

1. Internal Access Point (Limited customization like Logo and Background Image)
2. **External Hotspot (External 3rd party Web/Cloud hosted captive portal, fully customized)**
3. cnMaestro (Semi customized portal, with additional features like SMS Authentication, Payment Gateways and Vouchers)

Authentication Methods:

1. Clickthrough (Portal page with a button to accept terms & conditions and get internet access)
2. **RADIUS (External Authentication server like, Windows NPS / IAS or Free RADIUS)**
3. LDAP (Authenticate using LDAP/Active Directory)
4. Local Guest Account (Single username /password stored on Access Point)

In this document, we will be specifically talking about **External Hotspot** integrating with on-premise cnMaestro to securely **POST** the user credentials to authenticate the user using **External RADIUS**

Since the secure **POST** needs installation of certificate and installing certificate in each AP's in a big deployment is not straightforward, we are providing the option to install certificate in a single point(cnMaestro) for the whole network. Another benefit is this option also opens up the flow where the external portal can directly **POST** to cnMaestro and have the login flow completely done between client and the external portal which gets ways the issues with cross origin requests which are getting slowly blocked on browsers.

---

## Feature Details

---

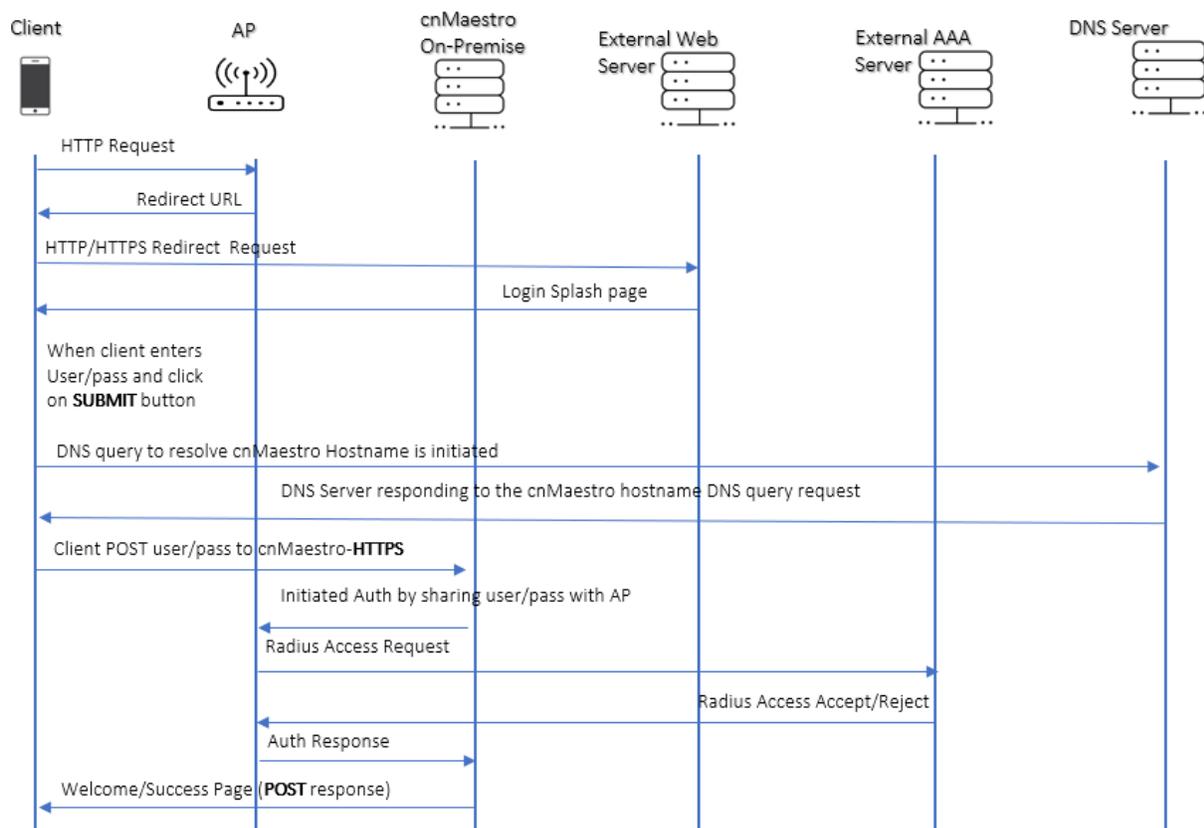
Customers who wanted a secure communication channel to authenticate the user securely should choose to POST the user credentials to cnMaestro. To enable this feature, one must enable **External Portal Post Through cnMaestro** available in Guest Access.

UI Screenshot:

External Portal Post Through cnMaestro

## Workflow

A general workflow when an external webserver and cnMaestro is configured to accept **HTTPS POST** messages from client.



This setup consists of below main parts:

1. Supplicant (Wireless clients- Laptops, mobile phones etc)
2. External Web Server
3. DNS server
4. On-Premise cnMaestro
5. Authenticator (Cambium Access Point)

---

## 6. Authentication Server (RADIUS)

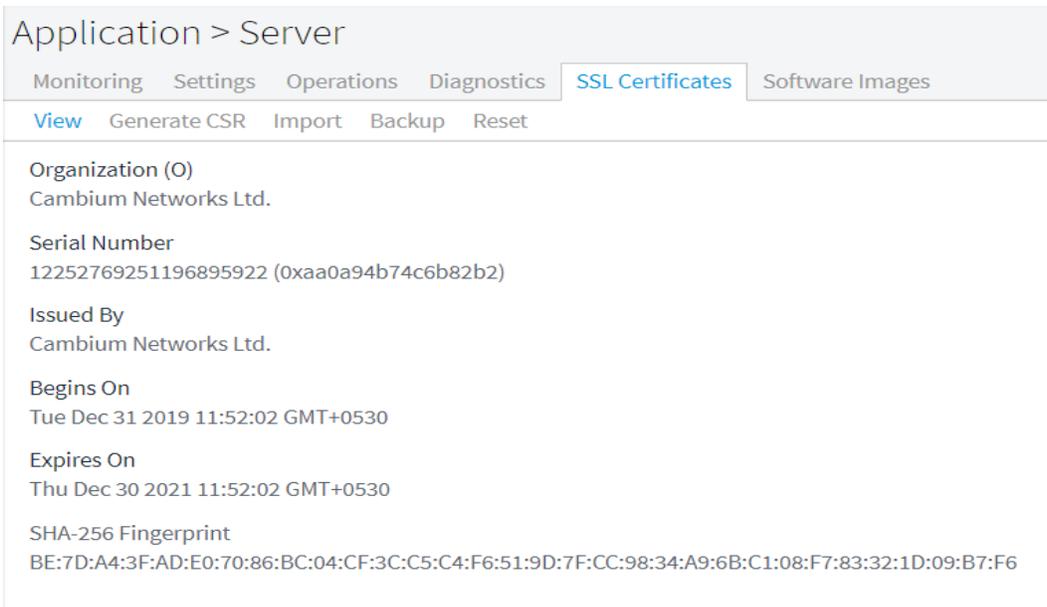
A certificate needs to be loaded on the cnMaestro for secure communication between clients and cnMaestro.

### 3<sup>rd</sup> party certificate loading on cnMaestro:

---

cnMaestro comes with a self-signed certificate. Customers would want this to change to a trusted certificate to provide the secure login page for their users.

*Self-signed certificate already available in the cnMaestro.*



The screenshot shows the 'Application > Server' configuration page. The 'SSL Certificates' tab is selected, and the 'View' button is active. The page displays the following information:

- Organization (O): Cambium Networks Ltd.
- Serial Number: 12252769251196895922 (0xaa0a94b74c6b82b2)
- Issued By: Cambium Networks Ltd.
- Begins On: Tue Dec 31 2019 11:52:02 GMT+0530
- Expires On: Thu Dec 30 2021 11:52:02 GMT+0530
- SHA-256 Fingerprint: BE:7D:A4:3F:AD:E0:70:86:BC:04:CF:3C:C5:C4:F6:51:9D:7F:CC:98:34:A9:6B:C1:08:F7:83:32:1D:09:B7:F6

Steps to load a 3rd party certificate on cnMaestro is as follows

1. Generate a CSR.

## Application > Server

Monitoring Settings Operations Diagnostics **SSL Certificates** Software Images

View **Generate CSR** Import Backup Reset

Generate a Certificate Signing Request (CSR) from the Private Key installed in cnMaestro. The CSR is used by a Certificate Auth Guest Access Portal without a warning.

Country (C)

India ▼

Common Name (CN)

wifi.cambiumnetworks.com

FQDN (fully qualified domain name) here.

Organization (O)

Cambium Networks

Organization Unit (OU)

Wi-Fi Guest Access

City/Locality (L)

Bangalore

State/Province (ST)

Karnataka

Subject Alternative Name (SAN)

DNS ▼

wifi.cambiumnetworks.com ⓘ

**Generate CSR**

2. Once the signed certificate is received from the 3rd party, load it onto the cnMaestro.

## Application > Server

Monitoring Settings Operations Diagnostics **SSL Certificates** Software Images

Options : View **Generate CSR** **Import** Backup Reset

Import a Signed Certificate generated from a CSR or a Signed Certificate along with its Key (optionally encrypted). For either choice, **please make sure all files (including Signed Certificate, Intermediate Certificates, and optional Key) are concatenated into a single PEM encoded file before uploading.** For certificate chaining bundle, the server certificate must appear before the chained certificates in the concatenated file.

**Import Signed Certificate from CSR**  Import Signed Certificate and New Key

3. After loading the certificate, change the guest portal's URL to reflect the new hostname.

## Services > Guest Access Portal

Guest Portal Hostname / IP

wifi.cambiumnetworks.com

Hostname is mandatory for social login.

Save

Note: DNS Server forward zone should be updated with an entry to point to the cnMaestro hostname. This will ensure that when client tries to contact the redirected URL (which AP provides to contact cnMaestro) external DNS can send a query response.

## Configuration

1. On cnPilot Access Points: Configure >> WLAN
2. On cnMaestro: Shared Settings/ WLANs and AP Groups >> WLANs

WLAN: Key in the **WLAN name** and **description**. By default, WLAN Name is taken as **SSID Name**.

WLANs > Guest\_WLAN

Configuration APs

**WLAN >**

- AAA Servers
- Guest Access
- Access Control
- Passpoint
- ePSK

**Basic Information**

Type\*  
cnPilot Enterprise (E-Series, ePMP Hotspot)

Name\*   
Guest\_WLAN

Description   
This is a Guest WLAN

AAA Server: Key in the AAA server setting like **IP address (RADIUS server)** and **shared secret** (This shared secret should match to the secret created on RADIUS server).

WLANs > Add New

WLAN

**AAA Servers >**

- Guest Access
- Access Control
- Passpoint
- ePSK

**Warning:** AAA Servers are configured separately for each WLAN.

Proxy RADIUS through cnMaestro

**Authentication Server**

| 1. Host  | Secret    | Port* | Realm |
|---|--|-------|-------|
| 10.110.200.100  | cambium  | 1812  |       |
|   |          | 1812  |       |
|   |          | 1812  |       |

Timeout  
3 Timeout in seconds for each request attempt (1-30)

Attempts  
1 Number of attempts before giving up (1-3)

Accounting Server

Advanced Settings

Guest Access: Enter the URL of captive portal hosted on external web server and select other required parameters.

### Example External page URL

1. IP address: [http://10.110.200.100:8000/login\\_cnMaestro.html](http://10.110.200.100:8000/login_cnMaestro.html)
2. URL : <https://dev.xyznetworkmanager.com/portal/index.php?hotspotname=laCambium>

Portal Page hosted on Webserver should perform a POST to cnMaestro from the client.

**NOTE: HTTPS POST to cnMaestro is supported only on the on-premise version.**

Login request must be sent to below URL over standard HTTPS port 443:

"https://cnMaestroHostName/cn-ctrl/ext-guest/ga-ext-login?<query\_string\_append>"

Logout request to be sent on below URL over standard HTTPS port 443:

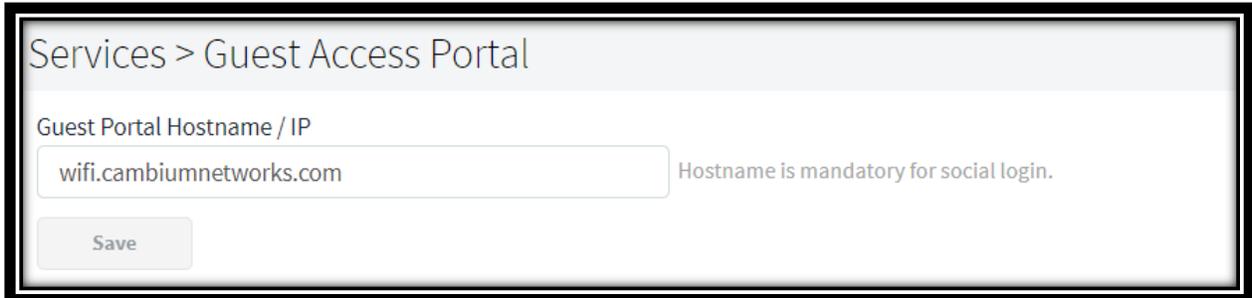
"https://cnMaestroHostName/cn-ctrl/ext-guest/ga-ext-logout<query\_string\_append>"

Please replace the cnMaestroHostName with the value as found in ga\_srvr query string in the redirection URL and add the same query string in this request.

---

The ga\_svr in the query strings points to the cnMaestro hostname/IP address what ever has been configured in the cnMaestro guest portal hostname config settings.

cnMaestro hostname can be found at cnMaestro Guest Portal settings



Here in this example configuration, the cnMaestro hostname is “**wifi.cambiumnetworks.com**”

Real time **POST** message for the above cnMaestro configuration is as follows

```
https://wifi.cambiumnetworks.com/cn-ctrl/ext-guest/ga-ext-  
login?ga_ssid=Guest_WLAN&ga_ap_mac=58-C1-7A-6E-DE-A1&ga_nas_id=E425-  
6EDEA1&ga_svr=wifi.cambiumnetworks.com&ga_cmac=E4-A7-A0-D4-31-  
C2&s=0wOu3Y7xiarhelDTFytHsAGQsGRkzRU2b_b5vh3GmNCl.&ga_Qv=eUROBR86HBgAGDEEVg  
QAGw4UWRUCACYVMgFPRy5ZXIFfUSVGWS9FVghZRyRLBhMUMww.
```

Note that, everything received as part of query string (everything after question mark) in the redirection URL, needs to be appended back in the POST URL.

## For deployments where cnMaestro hostname entry cannot be added to the DNS Server forward zone.

---

Note: IP reachability between the client and cnMaestro is must for client to **POST** the user credentials

- AP can be configured as a Proxy DNS to respond to the client’s DNS query.
- Only **CLI** support is added for this proxy feature.
- This is available from **3.11.4.1-r3** and **4.1-x**(yet to release) releases.

The commands should be added in Guest WLAN as below,

---

guest-access redirect user-page <cnMaestroIPAddress>  
guest-access redirect user-page hostname <cnMaestroHostname>

Example configuration screenshot:

```
E410-0DA1AF(config)#  
E410-0DA1AF(config)# wireless wlan 1  
E410-0DA1AF(config-wlan-1)#  
E410-0DA1AF(config-wlan-1)#  
E410-0DA1AF(config-wlan-1)# guest-access redirect user-page 10.110.200.83  
E410-0DA1AF(config-wlan-1)# guest-access redirect user-page hostname wifi.cambiumnetworks.com  
E410-0DA1AF(config-wlan-1)# save  
[Config Save OK]  
E410-0DA1AF(config-wlan-1)#
```

Guest WLAN CLI configuration screenshot:

```
wireless wlan 1  
  ssid Guest WLAN  
  no shutdown  
  vlan 1  
  security open  
  band both  
  dtim-interval 1  
  wpa-group-rekey-interval 3600  
  max-associated-client 127  
  network-policy-id 0  
  mac-authentication policy deny  
  radius-server authentication host 1 10.110.200.100  
  radius-server authentication secret 1 $crypt$1$Qpch6Ntr8Ziah02Oz1TNsdfqWSPhc603  
  radius-server called-sta-id AP-MAC:SSID  
  nas-identifier custom  
  radius-server rad-attr service-type 1  
  passpoint interworking access-network-type private  
  guest-access  
  guest-access access-type radius  
  guest-access redirect user-page 10.110.200.83  
  guest-access redirect user-page hostname wifi.cambiumnetworks.com  
  guest-access portal-mode external-hotspot http://10.110.200.100:8000/login_cnMaestro.html through-controller  
!  
E410-0DA1AF(config-wlan-1)#
```